UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/448,722	11/24/1999	BRUCE D. SUNSTEIN	2308/102	5379

2101 7590 07/13/2004

BROMBERG & SUNSTEIN LLP
125 SUMMER STREET
BOSTON, MA 02110-1618

EXAMINER	
REAGAN, JAMES A	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 07/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/448,722	SUNSTEIN ET AL.	
	Examiner	Art Unit	
	James A. Reagan	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 May 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. This action is in reply to the amendment and request for Continued Examination (RCE) received on 20 May 2004.

2. Claims 1, 2, 9, 17, 21, 22, 29-31, 36, 39, 41, 43, and 47 have been amended.

3. Claims 1-50 have been examined.

4. Claims 1, 2, 17, 29-31, 36 and 39 have been updated to reflect the amendments.

5. The rejections of the remaining claims are unchanged.

RESPONSE TO ARGUMENTS

6. Applicant's arguments received on 20 May 2004 have been fully considered but they are not persuasive. Referring to the previous Office action, Examiner has cited relevant portions of the references as a means to illustrate the systems as taught by the prior art. As a means of providing further clarification as to what is taught by the references used in the first Office action, Examiner has expanded the teachings for comprehensibility while maintaining the same grounds of rejection of the claims, except as noted above in the section labeled "Status of Claims." This information is intended to assist in illuminating the teachings of the references while providing evidence that establishes further support for the rejections of the claims.

With regard to the limitations of claims 1, 17, 29, 30, 31, 36, and 39, Applicant argues that *neither Pare, Bianco, Berson, nor the other art of record,*

alone or in combination, teach or otherwise suggest trusted databases for registration of personal information and user authentication. The Examiner asserts that Pare uses biometrics to control access to a user's bank account, and that Bianco uses biometrics to control access to enterprise resources and to specifically limit modification of the users personal information to the user. In addition, Applicant agrees that Bianco teaches a re-enrollment step that causes a modification of the physiological information of a users data set. Applicant further asserts that neither Bianco nor Pare disclose modification of a user's personal information. It is the professional opinion and position of this Examiner at the combination of Pare and Bianco discloses modification of personal information by utilizing physiologically-controlled access to a user's personal information. In support of this position, the Examiner uses Berson to teach a user modifying his own personal data while using biometric security protocols. It appears as if the Applicant is attacking the prior art reference piecewise instead of in combination as intended by the Examiner and shown in the rejections below under 35 U.S.C. 103(a). As shown, the combination of Pare, Bianco, and Berson discloses a system where in personal information may be modified by a particular user using physiological identifiers to authenticate the user.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pare Jr. et al. (U.S. Patent No. 6,154,879) and further in view of Bianco et al. (U.S. Patent No. 6,256,737), and further in view of Berson (US 6,532,459 B1).

Examiner's note: Examiner has pointed out particular references contained in the prior art of record in the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply. Applicant, in preparing the response, should consider fully the *entire* reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Claims 1 and 36:

Pare Jr. et al. shows, in figures 1-16 and related text, a method of administering registration of a personal information in a data base in a manner tending to assure integrity of data therein, the method comprising: obtaining, from each user with respect to whom data is to be placed in the data base, personal information of such user, the content of such personal information initially established by such user in an enrollment phase (column 13, lines 14-17); also

obtaining in the enrollment phase a first set of physiological identifiers associated with such user (column 3, lines 43-46; column 13, lines 10-12); storing, in digital storage medium, a data set pertinent to such user, the data set including such user's personal information and a representation of the physiological identifiers associated with such user (Fig 2); permitting a subject to modify information in the stored data set pertinent to such user (column 5, lines 11-13)

Pare Jr. et al. fails to explicitly show the user information can be modified only if (i) the subject provides a new set of physiological identifiers and (ii) it is determined, by recourse to the stored data set, that there is a sufficient match between at least one member in the new set and a corresponding member of the first set, so that the subject is authenticated as such user. Bianco et al. shows, in figures 1-34 and related text, in an analogous art related to the utilization of biometric measurements for the authentication of users, permitting a subject to modify information in the stored data set pertinent to such user only if the subject provides a new set of physiological identifiers and it is determined, by recourse to the stored data set, that there is a sufficient match between at least one member in the new set and a corresponding member of the first set, so that the subject is authenticated as such user (column 29, lines 5-10). Bianco et al. states that the biometric system (Fig. 1) including the re-enrollment step can be usefully incorporated into banking and financial transaction systems (e.g. ATM machines) (Bianco, column 58, lines 5-14) therefore, it would have been obvious, at the time

of the invention, to incorporate the re-enrollment step of Bianco into the biometric ATM access system of Pare.

The combination of Pare/Bianco does not specifically disclose that the integrity of a registration system is maintained by permitting modification of a particular user's personal information only by that user, using physiological identifiers to authenticate the user. Berson, however, in column 2, lines 28-67, discloses a user modifying his own personal data, and in column 5, lines 12-33, disclose biometric security protocols. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Pare/Bianco with Berson, because allowing an individual to update and otherwise modify their own personal data while ensuring a high-degree of security through the sue of biometric authentication helps prevent the fraudulent and criminal misuse of personal data.

With regard to the newly added limitations, the combination as shown above adequately disclose the authentication of the specified user allows the specified user to alter his or her own personal information contained within the database.

Claim 2:

Pare Jr. et al. shows, in figures 1-16 and related text, medical information is a suitable alternative type of data to credit and debit account numbers (column 2, lines 40-48). Therefore it would have been obvious to one of skill in the art, at the time of the invention to replace the account numbers obtained from the user

and stored in the data set (column 13, lines 14-30) with the medical information because choosing a suitable alternative from a known list of alternatives is common and well known in the art. Pare Jr. et al. fails to explicitly show the user information can be modified only if (i) the subject provides a new set of physiological identifiers and (ii) it is determined, by recourse to the stored data set, that there is a sufficient match between at least one member in the new set and a corresponding member of the first set, so that the subject is authenticated as such user. Bianco et al. shows, in figures 1-34 and related text, in an analogous art related to the utilization of biometric measurements for the authentication of users, permitting a subject to modify information in the stored data set pertinent to such user only if the subject provides a new set of physiological identifiers and it is determined, by recourse to the stored data set, that there is a sufficient match between at least one member in the new set and a corresponding member of the first set, so that the subject is authenticated as such user (column 29, lines 5-10). Bianco et al. states that the biometric system (Fig. 1) including the re-enrollment step can be usefully incorporated into banking and financial transaction systems (e.g. ATM machines) (Bianco, column 58, lines 5-14) therefore, it would have been obvious, at the time of the invention, to incorporate the re-enrollment step of Bianco into the biometric ATM access system of Pare.

With regard to the newly added limitations, the combination as shown above adequately disclose the authentication of the specified user allows the

specified user to alter his or her own personal information contained within the database.

Claim 3:

Pare Jr. et al. shows, in figures 1-16 and related text, a method according to claim 1, wherein the first set includes a plurality of members (column 13, line 10).

Claim 4:

Pare Jr. et al. shows, in figures 1-16 and related text, a method according to claim 1, wherein the first set of physiological identifiers includes the appearance of such user's face (column 26, lines 42-44).

Claim 5:

Pare Jr. et al. shows, in figures 1-16 and related text, a method according to claim 1, wherein the first set of physiological identifiers includes characteristics of utterances of such user (column 5, lines 22-25).

Claim 6:

Pare Jr. et al. shows, in figures 1-16 and related text, a method according to claim 1, wherein the first set of physiological identifiers includes a fingerprint of such user (column 5, lines 22-25).

Claim 7:

Pare Jr. et al. shows, in figures 1-16 and related text, a method according to claim 1, wherein the first set of physiological identifiers includes the configuration of an iris in an eye of such user (column 5, lines 22-25).

Claim 8:

Pare Jr. et al. substantially discloses the invention as claimed but does not explicitly show the first set includes at least one member selected from the group consisting of a fingerprint of such user and an configuration of an iris in an eye of such user and at least one member selected from the group consisting of characteristics of utterances of such user and the appearance of such user's face. Bianco et al. shows, in figures 1-34 and related text, in an analogous art related to the utilization of biometric measurements for the authentication of users, first set includes at least one member selected from the group consisting of a fingerprint of such user and an configuration of an iris in an eye of such user and at least one member selected from the group consisting of characteristics of utterances of such user and the appearance of such user's face (Fig 15). The layering of biometric devices, as shown in Bianco, provides flexibility to apply the appropriate level of protection to each resource without decreasing of network productivity (column 29, line 60 – column 30, lines 14).

Claim 9:

Bianco et al. shows, in figures 1-34 and related text, a method according to claim 1, wherein, pursuant to step (d), a subject is permitted to modify information in the sorted data set only if the subject provides the new set of physiological identifiers under a condition permitting verification, independent of the physiological identifiers, that the new set is being provided by the person purporting to provide them (column 28, line 43- column 29, line 39).

Claim 10:

Bianco et al. shows, in figures 1-34 and related text, wherein the condition includes the physical presence of the subject when providing the new set (column 29, lines 1-10).

Claim 11:

Bianco et al. shows, in figures 1-34 and related text, wherein the condition includes having the subject provide the new set when prompted to do so (column 29, lines 1-10).

Claim 12:

Bianco et al. shows, in figures 1-34 and related text, wherein the condition includes having the subject provide a non-physiological identifier (column 29, lines 1-10).

Claim 13:

Bianco et al. shows, in figures 1-34 and related text, wherein the non-physiological identifier is selected from the group consisting of a password and a pass card (column 29, lines 1-10).

Claim 14:

Bianco et al. shows, in figures 1-34 and related text, wherein the non-physiological identifier is provided in the course of a session, over a computer network, employing a user's public and private keys (column 51, lines 2-4; column 50, lines 35-47).

Claim 15:

Bianco et al. shows, in figures 1-34 and related text, prompting each user, on a periodic basis, to update the data set pertinent of such user (column 28, lines 43-52).

Claims 16 and 39:

Pare Jr. et al. shows, in figures 1-16 and related text, a method for authenticating a user transaction, the method comprising: obtaining a test set of physiological identifiers from a subject purporting to be a specific user (column 3, lines 43-46); accessing information in the data set pertinent to the specific user stored in accordance with the method of claim 1 (column 3, lines 51-55); and determining if there is a sufficient match between at least one member in the test set and a corresponding physiological identifier represented in the data set (column 3, lines 51-55).

With regard to the newly added limitations, the combination as shown above adequately disclose the authentication of the specified user allows the specified user to alter his or her own personal information contained within the database.

Claim 17:

Pare Jr. et al. shows, in figures 1-16 and related text, 17 a method for authenticating a user transaction, the method comprising: obtaining a test set of physiological identifiers from a subject purporting to be a specific user (column 3, lines 43-46; column 13, lines 10-12); accessing information in a first data set

pertinent to the specific user stored in a registration data base, the data base containing information provided by multiple users in a separate data set for each user, each data set of a specific user (Fig 2; column 3, lines 50-59) including (i) personal information, of the specific user, that has been established by the specific user, and (column 13, lines 13-16) (ii) a representation of a first set of physiological identifiers, associated with the specific user, that has been provided by the specific user (column 13, lines 10-14),; determining if there is a sufficient match between at least one member in the test set and a corresponding physiological identifier represented in the data set (column 3, lines 51-59).

Pare fails to show the data base being maintained under conditions wherein modification by a subject of information in a stored data set pertinent to the specific user is permitted only if (i) the subject provides a new set of physiological identifiers and (ii) it is determined, by recourse to the stored data set, that there is a sufficient match between at least one member in the new set and a corresponding member of the first set, so that the subject is authenticated as the specific user. Bianco et al. shows, in figures 1-34 and related text, in an analogous art related to the utilization of biometric measurements for the authentication of users, the data base being maintained under conditions wherein modification by a subject of information in a stored data set pertinent to the specific user is permitted only if (i) the subject provides a new set of physiological identifiers and (ii) it is determined, by recourse to the stored data set, that there is a sufficient match between at least one member in the new set and a

corresponding member of the first set, so that the subject is authenticated as the specific user (column 29, lines 5-10).

The combination of Pare/Bianco does not specifically disclose that the integrity of a registration system is maintained by permitting modification of a particular user's personal information only by that user, using physiological identifiers to authenticate the user. Berson, however, in column 2, lines 28-67, discloses a user modifying his own personal data, and in column 5, lines 12-33, disclose biometric security protocols. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Pare/Bianco with Berson, because allowing an individual to update and otherwise modify their own personal data while ensuring a high-degree of security through the sue of biometric authentication helps prevent the fraudulent and criminal misuse of personal data.

With regard to the newly added limitations, the combination as shown above adequately disclose the authentication of the specified user allows the specified user to alter his or her own personal information contained within the database.

Claim 18:

Pare Jr. et al. shows, in figures 1-16 and related text, the database is accessible via a server at a first location (Fig. 1); obtaining the test of physiological identifiers is performed at a second location remote from the first location (column 5, lines 1-3, Fig. 3); determining if there is a sufficient match

includes communicating with the server from the second location over a network (column 9, lines 25-27).

Claim 19:

Pare Jr. et al. substantially discloses the invention as claimed but fails to show obtaining the test set of physiological identifiers is performed under supervision of a merchant. Bianco et al. shows, in figures 1-34 and related text, in an analogous art related to the utilization of biometric measurements for the authentication of users, obtaining the test set of physiological identifiers is performed under supervision of a merchant (column 29, lines 15-21). Employing an administrator (merchant) to oversee the enrollment of a user helps ensure that the user enrolling is really the right person (column 28, lines 42-53). Therefore, it would have been obvious at the time of the invention to include the administrator of Bianco in the biometric ATM access system of Pare.

Claim 20:

Bianco et al shows determining if there is a sufficient match is performed without revealing content of the first data set to the merchant (column 28, lines 42-53).

Claims 21-28:

21-28, Pare Jr. et al. substantially discloses the invention as claimed but fails to show the transaction is a change of address for an account, is an application to open an account, the account authorizes the transfer of funds, the account is based on the extension of credit to the account holder, the transaction

is an application to a government agency for one of a license and a renewal of a license, the transaction is an application to a government agency for one of a license and a renewal of a license. It would have been obvious to one of skill in the art at the time of the invention to make the transaction a change of address for an account, an application to open an account, an application to a government agency for one of a license and a renewal of a license, an application to a government agency for one of a license and a renewal of a license or to make the account based on the extension of credit to the account holder because of these transactions are well known in the art to require user verification and the invention of Bianco describes a method of verifying a user.

Claim 29:

Pare Jr. et al. shows, in figures 1-16 and related text, a digital storage medium on which has been recorded a multi-user personal information data base, the data base comprising, for each specific user, a data set pertinent to the specific user (column 3, lines 39-43), the data set including: the specific user's personal information obtained from the specific user (column 3, lines 39-43); a representation of a first set of physiological identifiers associated with the specific user (column 3, lines 43-46); the user's emergency information obtained from the specific user (column 2, lines 40-48). Pare Jr. et al fails to show the storage medium being maintained under conditions wherein modification by a subject of information is a stored data set pertinent to the specific user is permitted only if (i) the subject provides a new set of physiological identifiers and (ii) it is determined,

by recourse the stored data set, that there is a sufficient match between at least one member in the new set and a corresponding member of the first set, so that the subject is authenticated as the specific user. Bianco et al. shows, in figures 1-34 and related text, in an analogous art related to the utilization of biometric measurements for the authentication of users, the storage medium being maintained under conditions wherein modification by a subject of information in a stored data set pertinent to the specific user is permitted only if (i) the subject provides a new set of physiological identifiers and (ii) it is determined, by recourse the stored data set, that there is a sufficient match between at least one member in the new set and a corresponding member of the first set, so that the subject is authenticated as the specific user (column 29, lines 5-10). Bianco et al. states that the biometric system (Fig. 1) including the re-enrollment step can be usefully incorporated into banking and financial transaction systems (e.g. ATM machines) (Bianco, column 58, lines 5-14) therefore, it would have been obvious, at the time of the invention, to incorporate the re-enrollment step of Bianco into the biometric ATM access system of Pare.

The combination of Pare/Bianco does not specifically disclose that the integrity of a registration system is maintained by permitting modification of a particular user's personal information only by that user, using physiological identifiers to authenticate the user. Berson, however, in column 2, lines 28-67, discloses a user modifying his own personal data, and in column 5, lines 12-33, disclose biometric security protocols. It would have been obvious to one of

ordinary skill in the art at the time of the invention to combine Pare/Bianco with Berson, because allowing an individual to update and otherwise modify their own personal data while ensuring a high-degree of security through the sue of biometric authentication helps prevent the fraudulent and criminal misuse of personal data.

With regard to the newly added limitations, the combination as shown above adequately disclose the authentication of the specified user allows the specified user to alter his or her own personal information contained within the database.

Claim 30:

Pare Jr. et al. shows, in figures 1-16 and related text, a system for updating a personal information database containing a data set for each one of multiple users (column 3, lines 39-43), each data set including a user's personal information and a representation of a first set of physiological identifier associated with the user (column 3, lines 39-43), the system comprising: a physiological identifier associated with a subject (column 3, lines 43-46); a user access authorization module, coupled to the physiological identifier transducer (column 5, lines 22-25), the database, for determining whether the output of the physiological identifier transducer sufficiently matches the representation of the first set of physiological identifiers, so that the subject is authenticated as the user (column 3, lines 43-54); a user data set access module, coupled to the user access authorization module and to the database, for accessing the user data set

(column 5, lines 10-12); a user data set update module, coupled to the database and to a user input, permitting the user to update such user's corresponding data set in the database (column 5, lines 10-12). Pare Jr. et al fails to explicitly show that the user access authorization module has authenticated the subject and the user prior to accessing the user data set. Bianco et al. shows, in figures 1-34 and related text, in an analogous art related to the utilization of biometric measurements for the authentication of users, the user access authorization module has authenticated the subject and the user prior to accessing the user data set (column 5, lines 10-12). Bianco et al. states that the biometric system (Fig. 1) including the re-enrollment step can be usefully incorporated into banking and financial transaction systems (e.g. ATM machines) (Bianco, column 58, lines 5-14) therefore, it would have been obvious, at the time of the invention, to incorporate the re-enrollment step of Bianco into the biometric ATM access system of Pare.

The combination of Pare/Bianco does not specifically disclose that the integrity of a registration system is maintained by permitting modification of a particular user's personal information only by that user, using physiological identifiers to authenticate the user. Berson, however, in column 2, lines 28-67, discloses a user modifying his own personal data, and in column 5, lines 12-33, disclose biometric security protocols. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Pare/Bianco with Berson, because allowing an individual to update and otherwise modify their own

personal data while ensuring a high-degree of security through the sue of biometric authentication helps prevent the fraudulent and criminal misuse of personal data.

With regard to the newly added limitations, the combination as shown above adequately disclose the authentication of the specified user allows the specified user to alter his or her own personal information contained within the database.

Claim 31:

Pare Jr. et al. shows, in figures 1-16 and related text, a system for authenticating transactions, the system comprising: a multi-user personal information data base, the data base comprising, for each specific user, a data set pertinent to the specific user (column 3, lines 39-43), the data set including: (i) personal information, of the specific user, that has been established by the specific user (column 3, lines 39-43); (ii) a representation of a first set of physiological identifiers, associated with the specific user, that has been provided by the specific user (column 3, lines 43-46); a multiplicity of remotely distributed terminals in communication with the data base, each terminal including a physiological identifier transducer and a communication link with a merchant (column 5, lines 1-5 & 19-33); an authenticity checker, which determines whether there is a sufficient match between the output of the a physiological identifier in the first set (column 3, lines 50-55). Pare Jr. et al. fails to explicitly show the data base being under condition wherein modification by a subject of information in a

stored data set pertinent to the specific user is permitted only if (i) the subject provides a new set of physiological identifiers and (ii) it is determined, by recourse to the stored data set, that there is a sufficient match between at least one member in the new set and a corresponding member of the first set, so that the subject is authenticated as the specific user. Bianco et al. shows, in figures 1-34 and related text, in an analogous art related to the utilization of biometric measurements for the authentication of users, the data base being under condition wherein modification by a subject of information in a stored data set pertinent to the specific user is permitted only if (i) the subject provides a new set of physiological identifiers and (ii) it is determined, by recourse to the stored data set, that there is a sufficient match between at least one member in the new set and a corresponding member of the first set, so that the subject is authenticated as the specific user (column 29, lines 5-10). Bianco et al. states that the biometric system (Fig. 1) including the re-enrollment step can be usefully incorporated into banking and financial transaction systems (e.g. ATM machines) (Bianco, column 58, lines 5-14) therefore, it would have been obvious, at the time of the invention, to incorporate the re-enrollment step of Bianco into the biometric ATM access system of Pare.

The combination of Pare/Bianco does not specifically disclose that the integrity of a registration system is maintained by permitting modification of a particular user's personal information only by that user, using physiological identifiers to authenticate the user. Berson, however, in column 2, lines 28-67,

discloses a user modifying his own personal data, and in column 5, lines 12-33, disclose biometric security protocols. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Pare/Bianco with Berson, because allowing an individual to update and otherwise modify their own personal data while ensuring a high-degree of security through the sue of biometric authentication helps prevent the fraudulent and criminal misuse of personal data.

With regard to the newly added limitations, the combination as shown above adequately disclose the authentication of the specified user allows the specified user to alter his or her own personal information contained within the database.

Claim 32:

Pare Jr. et al. shows, in figures 1-16 and related text, the first set includes a plurality of members (column 13, line 10).

Claim 33:

Pare Jr. et al. substantially discloses the invention as claimed but does not explicitly show the first set includes at least one member selected from he group consisting of a fingerprint of the user and the configuration of an iris in an eye of the user and at least one member selected from the group consisting of characteristics of utterances of he user and the appearance of the user's face. Bianco et al. shows, in figures 1-34 and related text, in an analogous art related to the utilization of biometric measurements for the authentication of users, first

set includes at least one member selected from the group consisting of a fingerprint of such user and an configuration of an iris in an eye of such user and at least one member selected from the group consisting of characteristics of utterances of such user and the appearance of such user's face (Fig 15). The layering of biometric devices, as shown in Bianco, provides flexibility to apply the appropriate level of protection to each resource without decreasing of network productivity (column 29, line 60 – column 30, lines 14).

Claim 34:

Pare Jr. et al shows, in figures 1-16 and related text, obtaining personal information of such user includes obtaining data pertaining to one or more merchants (column 13, lines 13-16).

Claims 35, 37, and 40:

Pare Jr. et al shows, in figures 1-16 and related text financial information that may be in the data set is not limited to that of a particular banking or financial institution (column 13, lines 13-16).

Claim 38:

Pare Jr. et al shows, in figures 1-16 and related text discloses, "...DPC site acts as the registration site, for implementation simplicity..." (column 13, line 18).

Claims 41 and 42:

The combination of Pare/Bianco as shown above discloses administering registration of a personal information in a data base in a manner tending to

assure integrity of data and the utilization of biometric measurements for the authentication of users. Pare/Bianco do not disclose *retaining a representation of at least one of the new set of physiological identifiers, if there is an insufficient match,* and *providing access to the retained representation of the at least one of the new set of physiological identifiers by a law enforcement official.* However, Examiner takes **Official Notice** that it is old and well known to confiscate identifications and other official papers that are being used fraudulently and to then turn them over to the proper authorities such as, for example, in the case of a minor trying to purchase alcohol or trying to gain entry to and adult establishment, or in the case of an individual using a passport or visa belonging to someone else. In each of these cases, the documents are usually seized and the suspects are routinely handed over to the proper authorities.

9. Claims 43-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pare/Bianco further in view of Ginter et al. (US 6,185,683).

Claims 43 and 45:

The combination of Pare/Bianco as shown above discloses administering registration of a personal information in a database in a manner tending to assure integrity of data and the utilization of biometric measurements for the authentication of users. Pare/Bianco do not specifically disclose *permitting a third party of a specified kind to view but not modify the user's personal information in the stored data set without requiring such third party to provide a*

physiological identifier that sufficiently matches a corresponding member of the first set of physiological identifiers stored in the data set. Ginter, however, in column 8, lines 38-45 discloses, "Secure electronic controls can specify how an item is to be processed or otherwise handled (e.g., document can't be modified, can be distributed only to specified persons, collections of persons, organizations, can be edited only by certain persons and/or in certain manners..." It would have been obvious to combine Pare/Bianco with Ginter because allowing third-party persons or organizations to only view but not modify sensitive data provide a benefit of controlling the rights management and secure chain of handling and control, preventing fraudulent use of personal data.

Claim 44:

Pare Jr. et al shows, in figures 1-16 and related text, obtaining personal information of such user includes obtaining data pertaining to one or more merchants (column 13, lines 13-16).

Claim 46:

The combination of Pare/Bianco/Ginter as shown above discloses administering registration of a personal information in a database in a manner tending to assure integrity of data and the utilization of biometric measurements for the authentication of users. Pare/Bianco/Ginter do not specifically disclose that *the specified kind is a health care provider.* However, Bianco, in column 20, lines 16-32 discloses access to medical records and patient information, inherently disclosing that a health care provider needs access to such

information. It would have been obvious to combine Pare/Bianco/Ginter because allowing third-party persons or organizations such as health care providers access to patient data provides a benefit of controlling the rights management and secure chain of handling and control, while providing health care services.

Claims 47-50:

The combination of Pare/Bianco as shown above discloses administering registration of a personal information in a database in a manner tending to assure integrity of data and the utilization of biometric measurements for the authentication of users. Pare/Bianco do not specifically disclose the following, but Ginter does a shown:

- *providing, to each user, a token indicating that the user has provided information to the data base* (column 8, lines 15-22);
- *the token comprises a card* (column 8, lines 63-65);
- *the token includes an identifier that, when presented to the data base by a third party, enables such third party to access but not modify the user's information in the data base* (column 8, lines 63-65);
- *the identifier comprises a record number identifying the data set pertinent to such user* (column 41, lines 37-40).

As shown above, Ginter, in column 8, lines 38-45 discloses, "Secure electronic controls can specify how an item is to be processed or otherwise handled (e.g., document can't be modified, can be distributed only to specified

persons, collections of persons, organizations, can be edited only by certain persons and/or in certain manners..." It would have been obvious to combine Pare/Bianco with Ginter because allowing third-party persons or organizations to only view but not modify sensitive data provide a benefit of controlling the rights management and secure chain of handling and control, preventing fraudulent use of personal data.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **James A. Reagan** whose telephone number is **(703) 306-9131**. The examiner can normally be reached on Monday-Friday, 9:30am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **James Trammell** can be reached at (703) 305-9768.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the **Receptionist** whose telephone number is **(703) 305-3900.**

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

(703) 305-7687 [Official communications; including After Final communications labeled "Box AF"]

(703) 308-1396 [Informal/Draft communications, labeled "PROPOSED" or "DRAFT"]

Hand delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive, Arlington, VA, 7th floor receptionist.

JAR
29 June 2004